PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-171460

(43)Date of publication of application : 30.06.1997

(51)Int.Cl. G06F 9/06
G06F 9/06
G06F 12/14

(21)Application number : 07-331481

(22)Date of filing : 20.12.1995

(71)Applicant : HITACHI LTD

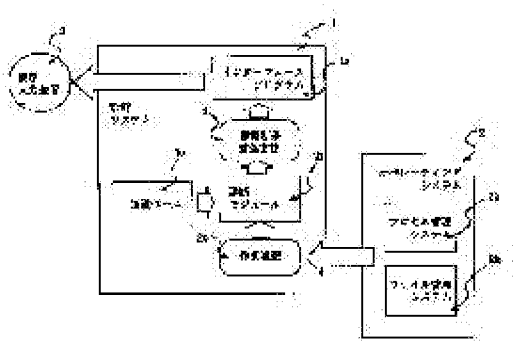
(72)Inventor : YOSHIDA KENICHI

(54) DIAGNOSTIC SYSTEM FOR COMPUTER

(57)Abstract:

PROBLEM TO BE SOLVED: To obtain a mechanism by which the fault such as installation mistake, etc., of a virus program is detected by comparing a stored operation and the actual state inside a computer.

SOLUTION: A knowledge base 1c stores the operation specification when a program is normal, the operation of the program when a program is infected with a virus program, etc., and the operation of the program when an installation mistake exists. A diagnostic module 1b compares the operations stored in the knowledge base 1c and the work history 2c that an operating system outputs, inspects the infection with the virus program and the installation mistake of the program and outputs the diagnostic results and a countermeasure 1d. Namely, the diagnostic module 1b compares the operation specification when the program is normal which is stored in the knowledge base 1c, and the work history 2c. When the both of them do not match with each other, it is judged that the program is infected with the virus or the installation mistake of the program exists and the diagnostic result is outputted.



* NOTICES *

JPO and INPIT are not responsible for any
damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]In this invention, the information about the programing operation which was not used, i.e., the related program call operation and file input/output operation of each program, is analyzed especially conventionally with respect to the obstruction detecting system of a computer.
Therefore, it is related with the structure which detects obstacles, such as an installation mistake of a virus program or a program.

[0002]
[Description of the Prior Art]Conventionally, infection of the virus program compared the contents of the file inside a computer with the program pattern which a virus program mainly has, and there was a virus check program which judges the existence of infection. In the installation mistake of the program, human being had mainly drawn diagnosis from operation of the computer.
[0003]In order to discover the invader from the outside as an analogous art, The action of a computer. The art to analyze. (For example, to "Detecting Intruders in Computer Systems", Teresa F.Lunt, 1993 Conference on Auditing and Computer Technology.) There was also a NIDES system described.
[0004]
[Problem(s) to be Solved by the Invention]The inspection of the virus program using the art enciphered in the above-mentioned conventional technology as a check program cannot judge a program pattern was difficult. The skilled expert attention was required for judgment of an installation mistake. NIDES was insufficient as a defense method to the virus which does damage quickly, in order to process the load information of CPU, etc. statistically.

[0005]The purpose of this invention is to provide the structure which detects obstacles, such as an installation mistake of a virus program or a program, by analyzing conventionally the information about the programing operation which was not used, in order to solve this problem.

[0006]
[Means for Solving the Problem]A database which memorized operation of a program in case the above-mentioned purpose has operation of a program at the time of being infected with operation specification, a virus program, etc. at the time of normal of a program, and an installation mistake, It is attained by preparing structure which observes a state inside a computer and comparing memorized operation with a actual state inside a computer.
[0007]
[Embodiment of the Invention]This invention is realized as the suitable database and program on a computer.
[0008]Hereafter, one example of this invention is described with reference to drawings.
[0009]Drawing 1 is a lineblock diagram of the computer system using this invention. 1 may be a diagnostic system for inspecting the installation mistake of infection of a virus program, or a program, and the suitable program on the computer which exchanges information with a computer application person using the display input device 3 may be sufficient as it. 1a may be an interface program of the diagnostic system 1, and the suitable program on a computer may be sufficient as it too. 2 may be an operating system of a computer and an operating system with the structure which outputs the information to which the program started the related program, and the information about the input/output operation which the program performed as the operation history 2c may be sufficient as it.
[0010]The operating system 2 with the mechanism in which a program outputs here the information which started the related program, and the information about the input/output operation which the program performed as the operation history 2c, It is easily realizable by giving a function required for the process management system 2a and file manager system 2b which are the sub programs inside an operating system. For example, if it is the UNIX operating system used by the computer of recent years many, it is easily realizable by giving a function required for the subroutine which realizes system calls, such as exec, fork, link, open, and close.
[0011]The knowledge base 1c is a database on the computer which memorizes operation of a program in case there are operation of the program at the time of being infected with operation specification, a virus program, etc. at the time of normal of a program and an installation mistake, and is one copy of the diagnostic system 1. The diagnostic module 1b compares the operation memorized to the knowledge base 1c with the operation history 2c which an operating system outputs, It is a program on the computer which inspects the installation

mistake of infection of a virus program, or a program, and outputs a diagnostic result and 1 d of solutions, and is one copy of the diagnostic system 1.

[0012]Here, when the operation specification and the operation history 2c at the time of normal of the program memorized to the knowledge base 1c are compared and both are not in agreement, the diagnostic module 1b is infected with the virus, or judges that there is an installation mistake of a program, and outputs 1 d of diagnostic results. When operation and the operation history 2c of the program at the time of being infected with the virus program etc. which were memorized to the knowledge base 1c are compared and both are in agreement, it judges that it is infected with the virus and 1 d of diagnostic results are outputted. When operation and the operation history 2c of a program in case there is an installation mistake memorized to the knowledge base 1c are compared and both are in agreement, it judges that there is an installation mistake of a program and 1 d of diagnostic results are outputted.

[0013]Drawing 2 is an example of processing inside the computer for explaining this invention, and the operating system 2 outputs the information on drawing 2 as the operation history 2c. In drawing 2, the user of a computer uses the application programs 4a, 4b, 4c, 4d, and 4e through the interface program 1a, The application programs 5a, 5b, 5c, and 5d were used through interface program 1a', and the application programs 6a, 6b, 6c, 6d, 6e, and 6f are used through interface program 1a."

[0014]Drawing 3 is an example of the normal operation of a program for explaining this invention, and is an example of the information memorized by the knowledge base 1c. If the source code of c program is created by the application program 6a (emacs), drawing 3, The created program is compiled by the application program 6e (cc) which the application program 6b (make) started, By being changed into the executable code application program 5c (prog.exe) by the application program 6f (ld), and a work process. The application program 6e (cc) the input file 7a (/usr/include/stdio.h), The application program 6f (ld) shows that the input file 7b (/usr/lib/libc.a etc.) is used as an input, and that the output file 7c (/tmp/work_file) is used as a file of operating.

[0015]Drawing 4 is an example of operation when the program for explaining this invention is infected with a virus, and is an example at the time of extracting one copy of contents of the operation history 2c. The difference from drawing 3 is operation of the application program 6f (ld). Although the application program 6f (ld) infected with the virus has tried writing to /os_image 8, If it compares with the example of normal operation of drawing 3, it can be diagnosed that it is what writing is not the original specification of the application program 6f (ld), and depends on infection of a virus this /os_image 8. When such unusual operation is caused, it can prevent generating a serious obstacle by a virus etc. by giving the function to suspend operation of an applicable program (in this case, KESHON program 6f) to the operating system 2. The function of this operating system 2 notifies that thing to the operating

system 2, when the diagnostic system 1 judges with "abnormal operation", and it can be easily realized by stopping the program from which the operating system 2 became an abnormality cause.

[0016]Drawing 5 is an example of a program when there is an installation mistake for explaining this invention of operation, and is an example at the time of extracting one copy of contents of the operation history 2c. If it compares with the example of normal operation of drawing 3, the input operation of the input files 7b, such as /usr/lib/libc.a by the application program 6f (ld) which should be essentially [this] successful, will go wrong (9a), As a result, it turns out that execution of the execute form program 5c (prog.exe) has gone wrong (9b). In such [conventionally] a case, a non-specialist understands only execution failure (9b) of the execute form program 5c (prog.exe), Although failure (9a) to the input of the input files 7b, such as /usr/lib/libc.a by the application program 6f (ld) which is the original cause, was not found, By comparing an example of operation, such an installation mistake (in this case, installation failure of a required file) can also be diagnosed.

[0017]In the above-mentioned example, since it was easy, explained noting that normal or unusual operation of the program was memorized by the knowledge base 1c, but. It is memorizing simultaneously the solution at the time of a viral infection and an installation mistake, and the solution which receives unusually [them] can also be outputted and it is an example of others of this invention.

[0018]Drawing 6 is a lineblock diagram of the example at the time of memorizing computer operation to the knowledge base 1c using this invention, and 1e is a knowledge base creation module. The state where a knowledge base creation module is not infected with 1. virus, but software is also normally installed in this example, And typical operation of the computer in the state where the inconvenience on installation was produced for the state with which the virus was infected for 2. knowledge base 1c creation, and 3. knowledge base 1c creation is memorized to ******-SU 1c.

[0019]Here, one copy with the suitable operation history 2c outputted from the operating system 2 may be sufficient as operation of the computer memorized by the knowledge base 1c. Here, the operation history 2c has a form of the graph illustrated to drawing 3, and 4 and 5 by making input/output relation of the file during a program into structural information. The state where it is not infected with 1. virus, but software is also normally installed if the pattern which appears repeatedly in this graph is extracted, And-izing of the typical operation of the state where the inconvenience on installation was produced for the state with which the virus was infected for 2. knowledge base 1c creation, and 3. knowledge base 1c creation, and each computer can be carried out [knowledge base].

[0020]Although extraction of the pattern which appears repeatedly in a graph may use what kind of technique, If the method shown in literature "extraction of the concept learning (1)

stereotyped reasoning process from a reasoning process, Yoshida and Motoda, Japanese Society for Artificial Intelligence, Vol. 7, No. 4, and pp.119-129" (1992) is used, It can include to the input/output relation isostructure information on the file during a program, a statistics value etc. can be analyzed, and the knowledge base 1c can be created based on an analysis result.

[0021]The computer which combines the example illustrated to drawing 1 and drawing 6, and enabled it to perform infection of a virus program etc., inspection of an installation mistake, and creation of the knowledge base 1c on the same machinery is also another example of this invention. In this case, by extracting a program pattern peculiar to the newly discovered virus together to the created knowledge base 1c, and memorizing it to it, The security of the system of structure which investigates the pattern of the virus as a character string memorized on the memory of the program which is conventional method can also be raised. That is, a computer presupposes during work that it was infected with a new type of virus with the computer system using this invention. Even if a virus tries to affect the operating system 2 by this invention, a motion of a virus is stopped safely and the knowledge base 1c about this virus can be created. By extracting a program pattern peculiar to the virus newly discovered at this time together, and memorizing it, the knowledge base for the systems of the mechanism of investigating the pattern of the virus as a character string memorized on the memory of the program which is conventional method can also be created. In this case, it can be inspected whether this program is infected with the virus by comparing with the program pattern extracted before starting a new program.

[0022]

[Effect of the Invention]The state inside a computer is compared with the operation which was memorized by the database in the above example according to this invention so that clearly, and infection and an installation mistake of a virus program etc. can be inspected according to a comparison result. Since the operation can be repealed when a computer starts the operation which is not normal, obstacles, such as destruction of the file by infection of a virus program, installation mistake, etc., are avoidable.

[0023]Since it diagnoses not in the pattern as a character string memorized on the memory of a program but in operation, the inspection of the virus program using the art enciphered as a check program cannot judge a program pattern is also possible. Since it is included in the operating system which is furthermore carrying out normal use, preparation of inspecting a virus with another device is also unnecessary, and the virus infected suddenly can also be coped with. The example which inspects a virus as compared with the operation pattern at the time of normal can respond also to the strange virus which operation does not understand.

[0024]Since the knowledge base about a strange virus can also be automatically created when the automatic creation also of the knowledge base further for diagnosis can be carried out and

* NOTICES *

JPO and INPIT are not responsible for any
damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1]A diagnostic system of a computer with structure which detects obstacles, such as a virus program, by having a database which memorized operation specification at the time of normal of a program, and the structure which observes a state inside a computer, and comparing operation specification at the time of normal with a state inside a computer.
[Claim 2]A diagnostic system of a computer with a mechanism of diagnosing an installation mistake of a program, etc. by having a database which memorized operation specification at the time of normal of a program, and the structure which observes a state inside a computer, and comparing operation specification at the time of normal with a state inside a computer.
[Claim 3]It has a database which memorized operation of a program at the time of being infected with a virus program etc., and the structure which observes a state inside a computer, A diagnostic system of a computer with structure which detects obstacles, such as a virus program, by comparing operation of a program at the time of being infected with a virus program etc. with a state inside a computer.
[Claim 4]By having a database which memorized operation of a program in case there is an installation mistake, and the structure which observes a state inside a computer, and comparing operation of a program in case there is an installation mistake with a state inside a computer, A diagnostic system of a computer with a mechanism of diagnosing an installation mistake of a program, etc.
[Claim 5]A computer system having the structure made into the invalidity of operation when it has a diagnostic system of a computer of a statement in either of above-mentioned claims 1 thru/or 4 and a computer starts operation which is not normal.
[Claim 6]A computer system having the structure which observes a state inside a computer and having a function which creates a knowledge base which memorized operation at the time of the time of normal and abnormalities of a program.

[Claim 7]In order to create a knowledge base which observed a state inside a computer and memorized operation at the time [normal] of a program and abnormalities, A computer system given in claim 6 paragraph including to input/output relation isostructure information on a file during a program, analyzing a statistics value etc., and creating a knowledge base based on an analysis result.

[Translation done.]